

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

INFORMATION ASSOCIATED WITH bigredd256@icloud.com
THAT IS STORED AT PREMISES CONTROLLED BY APPLE,
INC.

Case No. 4:23 MJ 8083 SRW

SIGNED AND SUBMITTED TO THE COURT
FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. 1073

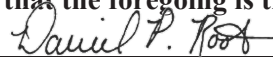
Unlawful Flight to Avoid Prosecution

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

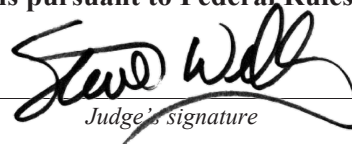

Applicant's signature

Daniel P. Root, Special Agent, FBI

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: April 14, 2023


Judge's signature

City and state: St. Louis, MO

Honorable Stephen R. Welby, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF)
INFORMATION ASSOCIATED WITH) No. 4:23 MJ 8083 SRW
bigredd256@icloud.com THAT IS STORED)
AT PREMISES CONTROLLED BY APPLE,)
INC.) FILED UNDER SEAL

**AFFIDAVIT IN SUPPORT OF
APPLICATIONS FOR SEARCH WARRANTS**

I, Daniel Root, a Special Agent with the **Federal Bureau of Investigation**, being first
duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 to require Apple Inc. (hereafter “Apple”), an electronic communications service/remote computing service provider, to disclose to the United States records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I have been employed as a Special Agent of the FBI since 2016 and am currently assigned to the FBI St. Louis Division. While employed by the FBI, I have investigated federal criminal violations related to matters involving the online sexual exploitation of children. I have gained experience through training at the FBI Academy, post Academy training, and everyday work related to conducting these types of investigations. I have conducted numerous investigations regarding the sexual exploitation of children that involve the use of the internet, computer devices

and cellular telephone to commit crimes such as violations of Title 18, United States Code, Sections 2251, 2252, 2252A, 2422 and 2423, which proscribe sexual exploitation of minors. I have been personally involved in the execution of search warrants to search residences and seize material relating to the sexual exploitation of minors including computers, computer equipment, software, and electronically stored information. I have experience utilizing computers during my career as an investigator and I have completed multiple in-service trainings, outside trainings to include SANS courses, and other courses in computer crime investigation.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1073 (unlawful flight to avoid prosecution) have been committed by Daniel Bert. There is also probable cause to search the location described in Attachment A for the information described in Attachment B for evidence of these crimes.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

LOCATION TO BE SEARCHED

6. The location to be searched is:

bigredd256@icloud.com (hereinafter referred to as “the target account(s)”) located at a premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

BACKGROUND INFORMATION RELATING TO APPLE ID AND iCloud¹

7. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

8. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

9. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

10. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

11. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on

Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

12. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

13. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to

communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

14. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

15. In some cases, account users will communicate directly with a Apple about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Apple typically retains records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

PROBABLE CAUSE

16. The United States, including the Federal Bureau of Investigation, is conducting a criminal investigation of Daniel BERT regarding the commission of the child exploitation offenses and his subsequent flight from prosecution.

17. On December 15, 2021, in the United States District Court, Eastern District of Missouri, Daniel BERT (BERT) was indicted by a grand jury and charged with a violation of Title 18, United States Code, Section 2252A(a)(1), Transporting Child Pornography. BERT self-surrendered to the FBI and United States Marshals Service on December 20, 2021.

18. On December 20, 2021, the United States District Court, Eastern District of Missouri, granted pre-trial release to BERT.

19. Thereafter, the United States Pretrial Services Office submitted numerous notices of BERT's alleged violations of his pretrial release, including on 4/13/22, 4/20/22, 5/2/22, 5/17/22, 6/10/22, 6/15/22, 8/9/22, 9/8/22, 10/9/22, and 11/21/22.

20. On December 9, 2022, United States Magistrate Judge Shirley P. Mensah issued a warrant for BERT's arrest following the submission of a Petition for Action on Conditions of Pretrial Release. In the petition, BERT's pretrial officer reported an in-home visit on 12/5/22 where open containers of alcohol and syringes were discovered in addition to an internet capable gaming system and a drone. BERT acted erratically, including uncontrollable shaking, randomly yelling, fidgeting and making sudden and quick movements. BERT's treatment counselor reported that BERT was not allowed to attend in a scheduled group session due to her belief that he was under the influence of an illicit substance. In addition, the FBI discovered that BERT was discovered to maintain an online OnlyFans account and that BERT had made an online post on June 19, 2022, while he was on bond.

21. On December 14, 2022, BERT was arrested pending a revocation hearing. On December 21, 2022, the Court held a status hearing to discuss BERT's medical condition, which involved him needing to be quarantined due to an infectious virus that posed a public health threat. Due to this diagnosis, the Court issued an Order of Temporary Release allowing BERT to be released to home incarceration and restricted to 24-hour-a-day lockdown at his residence (except for medical necessities and court appearances). BERT was also required to wear a GPS ankle monitor. BERT was further required to be evaluated by a licensed medical provider and obtain medical approval to be released from quarantine.

22. BERT was scheduled for a bond status hearing on January 27, 2023.

23. On January 15, 2023, BERT removed his court ordered GPS monitor and failed to respond to numerous attempts by his Pretrial Officer to contact him.

24. On January 17, 2023, the Court issued a warrant for BERT's arrest for numerous violations of his bond conditions, including absconding.

25. BERT's current whereabouts are unknown. Video surveillance obtained from BERT's apartment residence show BERT leaving his residence with a duffle bag and a suitcase on January 15, 2023. An unidentified male was with BERT.

26. Your affiant notes that, during the course of the criminal investigation, BERT used phone number 314-640-8118. The FBI received information from AT&T showing that BERT disconnected this phone number on or about January 15, 2023.

27. On January 19, 2023, the FBI served an administrative subpoena on Onlyfans.com or information related to user carhart256.² On February 17, 2023, Onlyfans.com provided a response to the administrative subpoena. The received response listed BERT, address 2206 Lucas

² Based on the criminal investigation, the FBI knows "carhart256" to be an online username previously used by BERT.

Avenue 414, St. Louis, Missouri 63103 and phone number (314) 704-3614. Investigators know 2206 Lucas Avenue #414 in St. Louis, Missouri to be a previous address for BERT.

28. Your Affiant applied for and was granted a search warrant for historical cellular tower data and call detail records for phone number (314) 704-3614. Analysis of the data returned from that search warrant shows that the handset travelled from St. Louis, Missouri, to Ft. Lauderdale, Florida in January 2023 before being deactivated.

29. The call detail records obtained through the search warrant also showed a high level of overlap with numbers that had been seen by your Affiant when reviewing call detail records from previous phone numbers known to be used by BERT.

30. This pattern is consistent with use of this cell phone number by BERT after his flight from St. Louis to avoid prosecution.

31. On March 15, 2023, Block, Inc. responded to FBI subpoena number 853735, which requested any account data associated with phone number (314) 704-3614.

32. The return from Block indicated that a CashApp account was associated with (314) 704-3614. On January 18, 2023, the e-mail for this account was changed to *bigredd256@icloud.com* (the **target account**).

33. The return also showed that an attempt was made to verify the user's identity using the names "Nicholas Pankratz" and "Nick Pankratz", which your affiant knows to be the name of BERT's deceased husband. The verification attempts were listed with results in the return as "FAILED_TO_VERIFY" and "DECEASED".

34. Based on the information provided in this affidavit, there is probable cause to believe that the target account is being used by BERT in furtherance of his violations of 18 U.S.C. § 1073 – Flight to Avoid Prosecution.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

35. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the United States copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

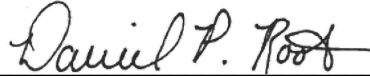
CONCLUSION

36. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

37. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.


38. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.



DANIEL ROOT
Special Agent
Federal Bureau of Investigation

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on April 14, 2023.



STEPHEN R. WELBY
United States Magistrate Court Judge
Eastern District of Missouri

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with *bigredd256@icloud.com* (the “target account”) that is stored at premises controlled by Apple Inc., a company headquartered at 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account(s) listed in Attachment A for the time period of 1 July 2022 to 11 April 2023:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);
- c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and

accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

- d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;
- e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);
- g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;
- h. All records pertaining to the types of service used; and
- i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken.
- j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within 14 days of the date of this warrant.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of 18 U.S.C. § 1073 involving Daniel BERT from 1 July 2022 to 11 April 2023, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS
PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND
902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **[PROVIDER]**, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **[PROVIDER]**. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **[PROVIDER]**, and they were made by **[PROVIDER]** as a regular practice; and

b. such records were generated by **[PROVIDER'S]** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **[PROVIDER]** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **[PROVIDER]**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature